UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/077,841	02/15/2002	Russell D. Housley	SPY-007-C1	3915

7590 06/14/2004

David R. Graham
1337 Chewpon Avenue
Milpitas, CA 95035

EXAMINER	
SMITHERS, MATTHEW	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/14/2004 9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/077,841	**Applicant(s)** HOUSLEY ET AL.
	Examiner Matthew B Smithers	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 04 April 2004 have been fully considered but they are not persuasive.

Applicant argues the combination of Chan, de Jong and Le does not teach the described advantageous characteristics found in applicant's specification from page 10, line 10 to page 11, line 3 where the value of the access permission data (block 403) cannot be changed once that value is stored in the data storage device. Applicant further discusses an example where a single mass produced cryptographic device can be configured to meet either the robust cryptographic capabilities of domestic regulations or the less robust cryptographic capabilities of the export regulations. Examiner contends, Le teaches manufacturing a single secure processing unit (cryptographic device) for domestic use that can be reconfigured after manufacture for use in foreign countries (see column 2, lines 41-57). Once the secure processing unit is reconfigured for export use, the value for the access permissions are set and cannot be changed in order to meet the export restrictions. Therefore, the combination does meet the limitation of configuring the data storage device after manufacture such that the value for the access permissions is set for the specific cryptographic device. Accordingly, the examiner maintains the rejection given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 9-14, and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,005,942 granted to Chan et al above, and further in view of U.S. patent 5,802,519 granted to De Jong and U.S. patent 5,883,956 granted to Le et al.

Regarding claim 1, Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). The operating system and security related code are stored in the ROM section (see column 1,line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing access permission data in the ROM section of the smart card. De Jong teaches a data structure for use in smart cards where access conditions (permissions) are stored in the memory means and are used to perform security measures (see column 8, lines 10-65 and column 12, lines 44-48). Neither Chan nor De Jong specifically teach the access permission data represents the availability of one or more cryptographic characteristics. Le teaches a secure processing unit embodied in a PersonCard (smart card) which uses a capability table that defines the cryptographic functions a secure processing unit can perform (see Abstract and column 7, line 50-et seq.) Le further shows the bit or bits within the capability table can specify the function or operating mode of a particular cryptographic operation, such as modulus size of the public-key pair or the allowable length of DES keys used by the particular function (see column 9, lines 19-58). It would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see **Le et al**; column 2, lines 41-57].

Regarding claim 2, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 1), in addition, Le teaches it is well known to use memory devices, such as programmable read-only memory (PROM) for storing system capability data (see column 3, lines 61-66 and column 7, lines 51-65).

Regarding claim 3, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 1), in addition, Le teaches permissible maximum length of DES key (see column 9, lines 32-58).

Claim 4 is a computer readable storage medium claim that is substantially equivalent to device claim 1. Therefore, claim 4 is rejected by a similar rationale.

Claim 18 is a computer readable storage medium claim that is substantially equivalent to device claim 2. Therefore, claim 18 is rejected by a similar rationale.

Regarding claim 5, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 4), in addition, Le teaches permissible maximum length of DES key (see column 9, lines 32-58).

Regarding claim 6, Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1,line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). It would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see **Le et al**; column 2, lines 41-57].

Regarding claim 9, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 6), in addition, Le teaches performing cryptographic operations, such as encryption/decryption using public or secret key algorithms (see column 7, lines 37-65).

Regarding claim 10, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 6), in addition, De Jong teaches storing sets of data in read-only memory (ROM)(see column 8, lines 14-52 and column 15, lines 15-51).

Regarding claim 11, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 10), in addition, De Jong teaches storing some of the second set of data in erasable programmable read-only memory (EEPROM)(see column 8, lines 14-52 and column 15, lines 15-51).

Regarding claim 12, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 11), in addition, De Jong teaches storing some of the second set of data in read-only memory (ROM)(see column 8, lines 14-52 and column 15, lines 15-51).

Regarding claim 13, Chan et al, De Jong and Le et al disclose everything claimed as applied above (see claim 6), in addition, De Jong teaches storing some of the second set of data in erasable programmable read-only memory (EEPROM)(see column 8, lines 14-52 and column 15, lines 15-51).

Claim 14 is a computer readable storage medium claim that is substantially equivalent to device claim 6. Therefore, claim 14 is rejected by a similar rationale.

Claim 17 is a computer readable storage medium claim that is substantially equivalent to device claim 9. Therefore, claim 17 is rejected by a similar rationale.

Regarding claim 19, Chan et al and De Jong disclose everything claimed as applied above (see claim 6), in addition, De Jong teaches controlling access between the various sets of data within the interaction contexts (see column 8, lines 14-52 and column 14, lines 19-29).

Claim 20 is a computer readable storage medium claim that is substantially equivalent to device claim 19. Therefore, claim 20 is rejected by a similar rationale.

Regarding claim 21, Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1,line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). It would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see **Le et al**; column 2, lines 41-57].

Claims 7, 8, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,005,942 granted to Chan et al above, and further in view of U.S. patent 5,802,519 granted to De Jong and U.S. patent 5,883,956 granted to Le et al and U.S. patent 3,962,539 granted to Ehrsam et al.

Regarding claim 7, Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1,line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device nor do either teach the sub-operations are comprised of one or more mathematical primitive operations. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). Ehrsam teaches a device for ciphering a block of data using a cipher key wherein the mathematical primitive operation includes a divide operation (see column 11, line 36-et seq) and an XOR operation (see column 20, lines 15-17 and Figures 3a, 3b, 3c, 3d, 3e, 3f, 3g, 3h, 3i, 3j and 8). It would have been obvious to one of ordinary skill in the art to combine the teachings of Ehrsam's product block cipher system for data security, Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card in order to provide the cryptographic designer with the details of how the key bits within the particular permutation are to be used for generating the keys for the specific cryptographic operation [see **Ehrsam et al**; column 2, line 32 to column 4, line 51].

Regarding claim 8, Chan et al, De Jong, Le et al and Ehrsam et al disclose everything claimed as applied above (see claim 7), in addition, Ehrsam teaches a divide operation (see column 11, line 36-et seq) and an XOR operation (see column 20, lines 15-17 and Figures 3a, 3b, 3c, 3d, 3e, 3f, 3g, 3h, 3i, 3j and 8).

Claim 15 is a computer readable storage medium claim that is substantially equivalent to device claim 7. Therefore, claim 15 is rejected by a similar rationale.

Claim 16 is a computer readable storage medium claim that is substantially equivalent to device claim 8. Therefore, claim 16 is rejected by a similar rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137